THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL **MOTION TO DISMISS COUNTS 2 THROUGH 8 OF THE SUPERSEDING INDICTMENT** Noted for January 14, 2022

I. INTRODUCTION

Defendant Paige Thompson, through counsel, moves the Court to dismiss Counts 2 through 8 in the superseding indictment with prejudice for a failure to state a claim, under Federal Rule of Criminal Procedure 12(b). Each of these counts allege that Ms. Thompson "intentionally accessed a computer without authorization" in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (a)(5)(A), but fail to provide a basis for their accusations. Ms. Thompson also moves to dismiss these counts because, as alleged, they violate her Fifth Amendment right to due process and First Amendment right to free speech and expression.

Counts 2 through 8 are legally defective, and those defects cannot be cured. First, the government cannot prove, as a matter of law, that Ms. Thompson's access of the Amazon Web Services ("AWS") servers rented by Capital One and the other entities was without authorization as required by the Computer Fraud and Abuse Act ("CFAA"). Second, the CFAA charges here are so novel and out of line with established precedent that they violate due process because Ms. Thompson could not have been aware that her alleged conduct violated the law. Third, the CFAA charges violate the First Amendment right to free speech and expression for participating in activities such as scripting code and receiving information that the owner of a computer makes publicly available. The Court should grant this motion and dismiss Counts 2 through 8 with prejudice.

II. RELEVANT FACTS

On June 17, 2021, the grand jury returned a superseding indictment ("Indictment"), which included ten counts.[1] Dkt. No. 102. Counts 2 through 8 charge Ms. Thompson with intentionally accessing a computer without authorization in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (a)(5)(A) (the "CFAA"). *Id.* at 5-8.

Count 1 (wire fraud) of the Indictment sets forth the government's vague theory with respect to Counts 2 through 8. That count alleges that Ms. Thompson utilized "proxy scanners" in an impermissible way. As stated in government's filings, these proxy scanners permitted Ms. Thompson to "scan the public-facing portions" of cloud servers owned and operated by AWS, but rented by Capital One and the other entities. The Indictment alleges that these proxy scanners allowed Ms. Thompson to "identify servers for which the web application firewall misconfigurations permitted commands sent from outside the servers." *Id.* at 3. According to the Indictment, once Ms. Thompson identified such misconfigurations, she "transmitted commands to the misconfigured servers that obtained the security credentials" belonging to Capital One and the other entities. *Id.* After Ms. Thompson obtained these security credentials, the Indictment alleges that she used them to obtain "lists or directories of folders or, buckets, of data," which she then copied to her own server; this data allegedly included

[1] The original indictment was filed on August 28, 2019, and included two counts charging wire fraud (Count 1) and violation of the CFAA (Count 2). Dkt. No. 33.

"personal identifying information, from approximately 100,000,000 customers who had applied for credit cards from Capital One." *Id.* at 4. The Indictment does not specify the data allegedly stolen from the other entities. *Id.* at 5.

In addition, the Indictment alleges that Ms. Thompson utilized the security credentials that she obtained to then impermissibly use the computing power of the AWS servers rented by Capital One and the other entities to mine cryptocurrency. According to the Indictment, Ms. Thompson attempted to use personally identifying information ("PII") taken from AWS's servers to create unauthorized credit and debit cards, and she intentionally and unlawfully possessed the PII of "millions of people." *Id*. at 5, 7-9.

As to Counts 2 through 5, the Indictment claims that the value of the information obtained by Ms. Thompson exceeded $5,000. *Id.* at 6-8. For Counts 6 and 7, the value of the information is not alleged. *Id*. at 7. For Count 8, the Indictment alleges that Ms. Thompson's alleged cryptocurrency mining cost certain entities a loss of over $5,000. *Id.* at 7-8. In sum, Counts 2 through 8 allege that Ms. Thompson violated the law by utilizing misconfigurations in the publicly facing portions of the web application firewalls of Capital One and the other entities and measure the harm by the value of the information allegedly obtained (Counts 2-5), the alleged damage caused by Ms. Thompson's purported cryptocurrency mining (Count 8), or not at all (Counts 6-7).

III. ARGUMENT

A. The Court Should Dismiss the CFAA Counts (Counts 2-8) Because They Fail to State a Legally Cognizable CFAA Claim.

Counts 2 through 8 of the Indictment are fatally flawed because the CFAA allegations do not amount to criminal activity. As such, the CFAA counts are ripe for dismissal with prejudice, even if read in a light most favorable to the government.

Rule 12(b) permits consideration of any defense, objection, or request "that the court can determine without a trial on the merits." Fed. R. Crim. P. 12(b)(1). A motion to dismiss pursuant to Rule 12(b) *must* be made before trial where the charging document lacks the requisite specificity or adequately fails to state an offense. *Id.* at 12(b)(3)(B). This Court and others in this Circuit have granted a defendant's motion to dismiss where such defects lay in the charging documents. *See, e.g., United States v. Webb*, 166 F. Supp. 3d 1198 (W.D. Wash. 2016) (dismissing Armed Career Criminal Allegation under Rule 12(b) because drug conspiracy convictions did not constitute predicate offenses) (Lasnik, J.); *United States v. Casey*, No. 2:20-CR-0020-RAJ, 2020 WL 1940446 (W.D. Wash. Apr. 22, 2020) (dismissing a count under Rule 12(b) after determining that a prior is not a habitual offense under 18 U.S.C. § 117(a)) (Jones, J.); *United States v. Thompson*, 202 F. Supp. 503 (N.D. Cal. 1962) (dismissing an indictment under Rule 12(b) after determining that a sawed-off shotgun without a firing pin was not a firearm within the National Firearms Act.).

The CFAA creates criminal liability for anyone who "intentionally accesses a computer" either (a) "without authorization" or (b) "exceeds authorized access," and thereby obtains particular information. 18 U.S.C. § 1030(a)(2); *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (emphasis added). The term "without authorization" is not defined in the statute, though the CFAA defines the term "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The Supreme Court clarified in *Van Buren* that the term "without authorization" turns on whether "one either can or cannot access a computer system." *Van Buren*, 141 S. Ct. at 1658; *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) (finding that court should look to the granting authority and the scope of the permission to understand whether a user acted without authorization). Authorization, in this context, means authentication, "which turns on whether a user's credentials allow h[er] to proceed past a computer's access gate." *Van Buren*, 141 S. Ct.. at 1659 n.9; *see United States v. Nosal ("Nosal II")*, 844 F.3d 1024, 1028 (9th Cir. 2016) (stating that "without authorization" is "an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."); *see also* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016) (noting that "authorization" necessarily implies the existence of an "authentication requirement" or some other mechanism "to create the necessary barrier that divides open spaces from closed spaces on the Web.")

To be liable under the CFAA, a defendant must enter a computer system, or files, folders, and/or databases on that computer system, "to which a computer user lacks access privileges." *Van Buren*, 141 S. Ct. at 1657-58; *see Domain Name Comm'n Ltd. v. DomainTools LLC*, 449 F. Supp. 3d 1024, 1027 (W.D. Wash. 2020) (Lasnik, J.) ("[O]ne is authorized to access a computer when the owner of the computer gives permission to use it."). The motive of the person accessing the computer information is irrelevant for purposes of the CFAA. *See Van Buren*, 141 S. Ct. at 1652 (holding that CFAA does not impose liability for someone who has "improper motives for obtaining information that is otherwise available to them"). Additionally, the CFAA does not distinguish among various means of access (*i.e.,* manual or automated), but rather whether the person accessing information has received the necessary authorization to do so. *See United States v. Nosal ("Nosal I")*, 676 F.3d 865, 857-59 (9th Cir. 2012) (distinguishing between unauthorized access to, and use of, data).

The "without authorization" clause of the CFAA "protects computers themselves by targeting so-called outside hackers—those who 'acces[s] a computer without any permission *at all*.'" *Van Buren*, 141 S. Ct. at 1658 (quoting *Brekka*, 581 F.3d 1127, 1133 (emphasis added). The “exceed[ing] authorized access” clause of the CFAA targets “so-called inside hackers—those who access a computer with permission, but then ‘exceed’ the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend.” *Van Buren*, 141 S. Ct. at 1658 (citing *United States v. Valle*, 807 F.3d 508, 524 (2d. Cir. 2015). Both clauses adopt “a gates-up-or-down approach.” *Id.* at 1659; *see DomainTools*, 449 F. Supp. 3d at 1027 (stating that whether access is authorized depends on the actions taken by the owner of the computer system).

Put another way, the CFAA prohibits “‘breaking and entering,’ where a defendant has unlawfully intruded into otherwise inaccessible computers (or portions thereof) in the form of trespass.” *DomainTools*, 449 F. Supp. 3d at 1029; *see Brekka*, 581 F.3d at 1133 (stating that, for purposes of the CFAA, once a computer has granted an individual authorization, it does not matter that such authorization might have been “subject to certain limitations”). Access to publicly available information, however, even information that may be publicly available inadvertently or through the abject neglect of its owner, is not “without authorization” under the CFAA.

Here, the Indictment fails to allege that Ms. Thompson committed “breaking and entering” into an otherwise inaccessible computer system. *See* Dkt. No. 102. Instead, the Indictment alleges that Ms. Thompson utilized scanners “to scan the public-facing portion of [AWS] servers” for “web application firewall misconfigurations” that “permitted commands sent from outside the servers to reach and be executed by the servers.” (*Id.* at 3.) Applying this same logic, anyone with a proxy scanner could have detected that some of the web application firewalls utilized by AWS customers were essentially “open gates.” As such, Ms. Thompson’s purported access of them should be no more liable under the CFAA than a person accessing a public-facing web page.

Once Ms. Thompson is alleged to have had access to the AWS servers, the Indictment claims she then "obtained the security credentials for particular accounts or roles belonging to the customers with the misconfigured servers" and obtained stored data utilizing those credentials. *Id.* at 3-4. These allegations are incredibly vague—they do not allege that any of the areas Ms. Thompson accessed were password protected or otherwise "unauthorized" once she was allegedly past the web application firewalls. They also do not state how Ms. Thompson obtained the security credentials other than that she "transmitted commands." *Id.* at 3. Most importantly, the Indictment fails to state how Ms. Thompson "obtained the security credentials," for example, by virtue of having made it past the web application firewall.

As a concrete example, if Ms. Thompson ran a "ListObjects" command once she made it past the web application firewall, and the AWS server executed the command for no other reason but for Ms. Thompson's actions, that would not constitute "unauthorized access" under *Van Buren* and subsequent decisions. *See Nosal I*, 676 F.3d at 864 (holding no CFAA liability where defendant obtained information from inside a database to which accomplices had access). This is because a verified user could have engaged in the same conduct and that person could be accused of violating the CFAA statutes in the same way that the Government accuses Ms. Thompson of being an unverified user. Because that scenario is entirely possible under the government's CFAA allegations in Counts 2 through 8, the allegations are infirm as a matter of law and the Court must dismiss these allegations. *See Van Buren*, 141 S. Ct. at 1659.

As it reads now, the Indictment attempts to charge Ms. Thompson with "hacking" for walking through an open door. That is a bold expansion of CFAA liability that is not supported by the case law and should be rejected by the Court. Under the government's theory of prosecution, so-called "white hat hackers," also known as computer security experts or "researchers" would also be liable under the CFAA every time they "breached" an open gate on the Internet and reported such to the company who left the gate open. That cannot, and should not, be the case. Capital One and the other entities left the gates to their rented AWS servers wide open to the public. As such, there can be no CFAA violation, and the Court should dismiss Counts 2 through 8 with prejudice.

B. The Court Should Dismiss the CFAA Counts (Counts 2-8) Because They Violate Ms. Thompson's Fifth Amendment Right to Due Process.

The government has pushed the boundaries of CFAA too far. The Fifth Amendment's right to due process protects Ms. Thompson from prosecution under Counts 2 thought 8, and provides an independent ground for dismissing Counts 2 through 8 with prejudice.

The government's use of the CFAA to claim that Ms. Thompson's alleged passage through an essentially open gate was a criminal violation of the CFAA is "surprising and novel" in a way that violates "the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed." *Brekka*, 581 F.3d at 1134-35 (citation omitted). The rule of lenity "requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government." *Id.* at 1135 (quoting *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006); *see Nosal I*, 676 F.3d at 863 ("The rule of lenity requires penal laws . . . to be strictly construed.") (citation omitted).

Penal statutes must "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). "Vagueness may invalidate a criminal law for either of two independent reasons": it may not provide fair notice as to the conduct prohibited or "it may authorize and even encourage arbitrary and discriminatory enforcement." *City of Chi. v. Morales*, 527 U.S. 41, 56 (1999); *accord Beckles v. United States*, 137 S. Ct. 886, 894 (2017). The government violates the Fifth Amendment's guarantee of due process when it "tak[es] away someone's life, liberty, or property under a criminal law so vague that it fails to give ordinary people fair notice of the conduct it punishes, or so standardless that it invites arbitrary enforcement." *Johnson v. United States*, 135 S. Ct. 2551, 2554 (2015) (citation and internal punctuation omitted); *accord Beckles*, 137 S. Ct. at 892. The government's novel argument as to the application of the CFAA to Ms. Thompson's actions in this matter are unconstitutionally vague and should be dismissed.

The Court should be especially mindful of an expansive reading of the CFAA because, as the Supreme Court cautioned, "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." *Van Buren*, 141 S. Ct. at 1661. In particular, the government's interpretation of the CFAA here has the potential to chill the actions of white hat hackers, which risks exposing "victims" such as Capital One to far *more* data breaches, not fewer. *See id.* at 1652 ("The Government's interpretation of the 'exceeds authorized access' clause would attach criminal penalties to a breathtaking amount of commonplace computer activity."); *Nosal I*, 676 F.3d at 863 ("If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [Nosal] engaged, then 'we must choose the interpretation least likely to impose penalties unintended by Congress.'") (citation omitted).

Here, the text of the CFAA statute is unconstitutionally vague and is void as applied to Ms. Thompson's alleged conduct. The text of the CFAA did not give Ms. Thompson "fair notice" that accessing a web application firewall that was essentially open to the public, as she is alleged to have done, was a federal crime. "A criminal statute must clearly define the conduct it proscribes. If it does not 'give a person of ordinary intelligence fair notice' of its scope, . . . it denies due process." *Bond v. United States*, 572 U.S. 844, 872 (2014) (Scalia, J., with justices Thomas and Alito, concurring in the judgment) (citation omitted). "No one should have to ponder the totality of the circumstances in order to determine whether his [or her] conduct is a felony." *Id.* at 873. "The principle is that no man [or woman] shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed." *United States v. Lanier*, 520 U.S. 259, 265 (1997) (quotation marks and ellipses omitted).

As discussed above, the *sine qua non* of a CFAA violation is lack of authorization in the sense that the person accessing the computer does not have authorization from that computer system or that computer system's owner and only manages to access that computer system through force (*i.e.,* "breaking and entering"). Nothing in the text of the CFAA, or the legal opinions that have interpreted it since its passage, would put a defendant such as Ms. Thompson on notice that utilizing a widely and publicly-available device such as a proxy scanner to detect "open gates" on servers connected to the Internet would subject her to criminal liability under the CFAA. This is especially so considering that Ms. Thompson allegedly engaged in the *exact* same behavior that "white hat" hackers engage in to notify companies of lapses in their computer security. Many corporations, including Capital One, reward "white hat" hackers with money for their multiple breaches of computer security utilizing the *very same* techniques purportedly undertaken by Ms. Thompson, yet Ms. Thompson was "rewarded" with a multiple count criminal indictment. That is not due process.

Additionally, the government's use of the CFAA to prosecute Ms. Thompson for behavior that is almost identical to that of a "white hat hacker" or "researcher" is unconstitutionally arbitrary. Due process requires that the "legislature establish minimal guidelines to govern law enforcement.'" *Kolender*, 461 U.S. at 358 (quoting *Smith v. Goguen*, 415 U.S. 566, 574 (1974)). "Laws that 'regulate persons or entities'. . . must be sufficiently clear 'that those enforcing the law do not act in an arbitrary or discriminatory way.'" *Beckles*, 137 S. Ct. at 894 (quoting *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012)). Where there are no minimal guidelines, a criminal statute may permit "a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections." *Smith*, 415 U.S. at 575; *accord Sessions v. Dimaya*, 138 S. Ct. 1204, 1212 (2018) (plurality). "The degree of vagueness that the Constitution tolerates - as well as the relative importance of fair notice and fair importance - depends in part on the nature of the enactment." *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 498 (1982). "For statutes involving criminal sanctions the requirement for clarity is enhanced." *United States v. Harris*, 705 F.3d 929, 932 (9th Cir. 2012) (ellipses and quotation marks omitted).

Stated simply, every day, numerous people in the technology industry and researchers around the country scan the internet, communicate with publicly facing websites, obtain information from the websites, and save the information on their computers. There is no other case reported or unreported in the country the defense has been able to locate where the CFAA has been applied in such a manner. The government has selected to prosecute Ms. Thompson, a transgender person with significant mental health issues, to the exclusion of other individuals who regularly engage in similar activities on the Internet, including "white hat" hackers. This prosecution is unconstitutionally arbitrary.

C. The Court Should Dismiss the CFAA Counts (Counts 2-8) Because They Violate Ms. Thompson's First Amendment Right to Free Speech and Expression

The First Amendment provides another separate basis for dismissal. Counts 2 through 8 raise First Amendment concerns for those who utilize publicly (and widely) available applications, such as proxy scanners, and write code designed to test, access, and even copy or "scrape" from publicly available data repositories and/or websites.

The First Amendment protects access to information as well as expressive activity. *See Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748, 756-57 (1976) ("[T]he protection afforded is to the communication, to its source and to its recipients both . . . . [T]his Court has referred to a First Amendment right to receive information and ideas, and that freedom of speech necessarily protects the right to receive.") (citations and internal quotation marks omitted). The First Amendment also protects the right to access the Internet generally. *Packingham v. N.C.*, 137 S. Ct. 1730, 1735, 1737 (2017). These "basic principles of freedom of speech" do not vary "when a new and different medium for communication appears." *Brown v. Entm't Merchs. Ass'n*, 564 U.S. 786, 790 (2011) (citation omitted); *see Citizens United v. Fed. Election Comm'n.*, 558 U.S. 310, 326 (2010) ("[D]eclin[ing] to draw, and then redraw, constitutional lines based on the particular media or technology used.")

As discussed above, what the CFAA criminalizes is the "breaking and entering" of protected computers by those who have *no* authorization to access the protected computers in the first place. *See Van Buren*, 141 S. Ct. at 1658. It does not—and constitutionally cannot—criminalize white hat hacking, data mining, scraping, and access to publicly available resources on the Internet. *See, e.g., Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 570 (2011) (upholding data miners' First Amendment right to access large amounts of information for analytics). There is a First Amendment expressive right to participate in those activities, particularly in scripting the code that is utilized in effectuating such activities, and a First Amendment right to receive information that the owner of a computer makes publicly available (whether the public nature of the material is purposeful or inadvertent does not change the First Amendment analysis). The government's CFAA charges, Counts 2-8, not only trample Ms.

Thompson's First Amendment rights because her alleged conduct falls within the protections of the First Amendment, but have the potential to chill the First Amendment rights of other white hat hackers, data miners, and scrapers across the Internet. This is unconstitutional and impermissible.

IV. CONCLUSION

For all of the above-stated reasons, the Court should dismiss Counts 2 through 8 of the Indictment with prejudice.

DATED: December 2, 2021

Respectfully submitted,

/s/ *Mohammad Ali Hamoudi*
MOHAMMAD ALI HAMOUDI
/s/ *Christopher Sanders*
CHRISTOPHER SANDERS
/s/ *Nancy Tenney*
NANCY TENNEY
Assistant Federal Public Defenders

/s/ *Brian Klein*
BRIAN KLEIN
/s/ *Melissa Meister*
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson